

Deep Packet Inspection:

THE END OF
THE INTERNET AS
WE KNOW IT?

M. Chris Riley
and Ben Scott
Free Press
March 2009

freepress 
www.freepress.net

TABLE OF CONTENTS

3	<i>Introduction</i>
4	<i>DPI History: Comcast and NebuAd</i>
4	Comcast and Internet Blocking
5	NebuAd and Internet Monitoring
6	<i>The Present Day: Prioritization on the Internet</i>
6	Cox Communications
6	Queuing Winners and Losers
7	Risks to Innovation and the Internet
9	ZillionTV: The Future of Discrimination?
10	<i>The Future: Monitoring and Monetizing Through DPI</i>
10	Marketing DPI to Internet Service Providers
13	DPI Shortchanges Consumers
15	<i>Endnotes</i>

INTRODUCTION

During the explosive rise of the Internet, one fundamental principle governed: All users and all content were treated alike. The physical network of cables and routers did not know or care about the user or the content. The principle of nondiscrimination, or “Net Neutrality,” allowed users to travel anywhere on the Internet, free from interference. Nondiscrimination, in various forms, has been a foundation of communications law and policy for decades.

In the early days of the Internet, nondiscrimination was easy to uphold because it was not technologically feasible for service providers to inspect messages and evaluate their content in real time. But recently, electronics manufacturers have developed so-called Deep Packet Inspection (DPI) technology capable of tracking Internet communications in real time, monitoring the content, and deciding which messages or applications will get through the fastest.

Here’s how it works: Messages on the Internet are broken down into small units called packets. Each packet contains a header and a data field. The header contains processing information, including the source and destination addresses. The data field contains everything else, including the identity of the source application (such as a Web browser request, a peer-to-peer transfer, or an e-mail), as well as the message itself (part of the contents of a Web page, file or e-mail). Packets are much like letters – the outside of the envelope is like the packet header, and the inside, like the data field, carries the message.

Historically, Internet communications were processed using only information in the header, because only that information is needed to transfer packets from their source to their destination. By contrast, DPI technology opens and reads the data field in real time, allowing network operators to identify and control, at a precise level, everyday uses of the Internet. Operators can tag packets for fast-lane or slow-lane treatment – or block the packets altogether – based on what they contain or which application sent them.

The first DPI devices were used for manual troubleshooting of network problems and to block viruses, worms and Denial of Service attacks. Initially, DPI was not powerful enough to monitor users’ Internet communications in real time. But today, DPI is capable of far more than security – it enables new revenue-generating capabilities through discrimination.

This new use of DPI is changing the game. In fact, improper use of DPI can change the Internet as we know it – turning an open and innovative platform into just another form of pay-for-play media. Although early uses of real-time DPI by ISPs have been geared toward targeted advertising and reducing congestion, manufacturers market the technology for its ability to determine and control every use of a subscriber’s Internet connection. When a network provider chooses to install DPI equipment, that provider knowingly arms itself with the capacity to monitor and monetize the Internet in ways that threaten to destroy Net Neutrality and the essential open nature of the Internet.

DPI HISTORY: COMCAST AND NEBUAD

The principle of nondiscrimination on the Internet has been codified in law in different ways over the past 20 years. In the first years of network technologies, when users connected to the Internet exclusively over telephone lines, the law of nondiscrimination was carried over from telephone regulations. The rules in place at the Federal Communications Commission prohibited “unjust and unreasonable discrimination” in the operation of phone service.¹ Known as “common carriage,” this regime governed network services for decades until the advent of broadband Internet access services led Congress and the FCC down another path.

Under intense pressure from incumbent phone and cable companies, the FCC moved ISPs out from under common carriage regulations, effectively lifting their nondiscrimination obligations.² But the FCC also issued an *Internet Policy Statement*, declaring that it would protect the rights of Internet users to access the content and attach the devices of their choice.³ The decision to swap out regulations for principles was based, in part, on assurances major broadband providers gave to the FCC that they would not discriminate.⁴ But soon after, network operators began to concoct plans to create new revenue streams by speeding up certain content at the expense of other content – in other words, discriminating.⁵ A major legislative debate followed in Congress – with cable and phone companies lining up on one side and public interest groups and Internet innovators on the other – as to whether to reinstate nondiscrimination rules (aka “Net Neutrality”) or to terminate them permanently. The outcome was a deadlock, leaving the *Internet Policy Statement* as the only remaining line of defense for Internet users.

COMCAST AND INTERNET BLOCKING

A series of events in 2007 led to a high-profile case at the FCC testing the strength of the *Internet Policy Statement*. It began when Comcast users started posting complaints on user message boards about the cable operator’s treatment of peer-to-peer traffic. Though no one could identify quite how it was happening, it appeared that Comcast was blocking file transfers between users. Robb Topolski, a network engineer in Portland, Ore., cracked the code with a series of experiments in the fall of 2007. Additional tests were done by Topolski, the Associated Press and the Electronic Frontier Foundation, which collectively determined that Comcast was using DPI technology to identify packets coming from peer-to-peer applications. Comcast was then secretly blocking those packets, while allowing other packets to pass through unimpeded. Comcast’s actions presented a clear case of network discrimination.

In November 2007, Free Press and other public interest organizations filed a petition with the FCC to demand that Comcast’s activities be stopped and ruled unlawful.⁶ After two public hearings, substantial media attention, and overwhelming public opposition to the practice, the FCC ruled against Comcast and ordered a halt to the company’s blocking practices.⁷ The ruling was a major victory for backers of Net Neutrality. However, the FCC’s order fell short of making Net Neutrality the unambiguous law of the land. The commission’s ruling found that ISPs could not block consumers from accessing online content – but it did not squarely address the underlying issue of discrimination that stopped short of blocking.

Following the commission’s order, Comcast stopped its peer-to-peer blocking practices and instituted a new network management system that does not discriminate against or in favor of any Internet applications.⁸ Comcast’s new system identifies neighborhoods that are growing substantially congested,

and then identifies individual users within those neighborhoods that are using a substantial amount of bandwidth, and slows down those heavy users for a short period of time.⁹ Although imperfect,¹⁰ Comcast has adopted a non-discriminatory network management regime that deals with congestion without attempting to pick winners and losers on the Internet.

NEBUAD AND INTERNET MONITORING

The dangers of DPI are not limited to violations of Net Neutrality; they extend to violations of privacy as well. Until its reorganization in 2008, a company called NebuAd offered an advertising service to network providers. With this service, NebuAd devices would secretly sit at key places within the network and monitor all consumer communications passing through the network, using DPI to search within packets for URLs and search terms. The devices would then analyze some or all of that traffic to identify consumer behavior patterns.¹¹ But NebuAd's activities went beyond information gathering. NebuAd artificially inserted packets of data into the stream of traffic to redirect Web browsers to a NebuAd-owned domain for the purpose of placing unsolicited tracking cookies on the user's computer.¹²

In March 2008, Internet users began detecting unsolicited cookies originating from NebuAd systems put in place by ISPs without notice.¹³ In May 2008, NebuAd made headlines by announcing a targeted advertising partnership with Charter Communications.¹⁴ After substantial pressure from public interest groups, subcommittees from both the House¹⁵ and the Senate¹⁶ held hearings to investigate the arrangement and NebuAd's practices. As a result of intense negative feedback from Congress and its customers, Charter terminated its arrangement with NebuAd in June 2008.¹⁷ The company has now virtually disappeared, but the enticing business of consumer tracking remains an attractive proposition for many ISPs.

In the cases of Comcast and NebuAd, consumer interests won the battle, though the war is far from over. The manufacturers of DPI equipment are committed to selling tools for network monitoring and discrimination, and were not deterred by the Comcast and NebuAd debacles. The debate over the use of DPI has only begun. Appropriate uses of DPI technologies do exist. But the applications we have seen thus far are not encouraging, and the burden of proof for their benefit rests squarely with the network operator.

THE PRESENT DAY: PRIORITIZATION ON THE INTERNET

COX COMMUNICATIONS

Despite the examples of Comcast and NebuAd, other providers are instituting discriminatory network management practices. The most high-profile of these is Cox Communications. Cox operates a cable network, which by design shares bandwidth among a large number of users. When the network becomes congested at peak usage times, the user experience suffers. Cable operators therefore have an incentive to figure out a way to manage traffic to ease the congestion by discouraging bandwidth-intensive uses of the network – thus avoiding further investment in physical network upgrades. In the short term, practices that target specific uses or users may well improve consumer experiences. But in the long term, these management practices may hurt innovation in high-bandwidth applications, reduce consumer choice and shackle the free market of Internet content and services.

Cox is currently engaging in trials of a new network management system that uses DPI to identify traffic from various Internet applications, and then chooses which applications deserve high priority and which can be slowed down. Cox has not deployed these systems across its network, but is currently testing them on subscribers in Kansas and Arkansas. Cox may be well-intentioned in trying to ensure that a congested network still performs well for users. But questions remain as to why the provider opted for this system rather than adopting the network management practices publicly disclosed by Comcast after the FCC decision. In contrast to Cox's system, Comcast's current network management practices slow down all traffic from high-bandwidth users, rather than traffic from specific high-bandwidth applications.¹⁸

If extended to a network-wide practice, Cox's network management system would set an alarming precedent that a service provider may choose how different applications are treated. This practice takes away user choice and threatens to diminish the innovation at the edges that has long made the Internet valuable. Although Cox may not choose to use that power for commercial purposes, business models designed to take advantage of discrimination will emerge. These future ramifications should be seriously considered in analysis of the Cox tests or of any other company in pursuit of similar activities.

QUEUING WINNERS AND LOSERS

Prioritization in the Cox system is performed through traffic queuing. Queuing is normal behavior on the Internet – every modern router has a queue. Ordinary network operation queues packets for a second or two during bursts of usage to maintain smooth and fast traffic flow. Default queues on the Internet operate under what is known as the “best efforts” model: The router forwards the packets at the front of the queue as fast as it can; if the queue is overwhelmed, some packets are lost. This is why the Internet is sometimes referred to as a “best efforts” network.

Although the full details have not been publicly disclosed, based on Cox's initial statements, Cox's new system splits the normal queue into two queues: “less time-sensitive” or low-priority traffic and “time-sensitive” or high-priority traffic.¹⁹ The system identifies the application from which the traffic originates through the use of DPI technology. It then selects a queue based on the time sensitivity

of the application, as determined by Cox. The system sends the traffic from the low-priority queue through the router less frequently than from the high-priority queue.

By placing the two types of traffic into separate queues in the router, Cox's system can speed up certain uses of the Internet at the expense of others. For example, Cox might choose to forward three packets from the low-priority queue for every seven it forwards from the high-priority queue. Another approach would be one in which the system sends any and all packets from the high-priority queue before sending any from the low-priority queue.²⁰ The result of either approach, from the user's perspective, is that some applications will work better than others. In some cases, the differences may not be perceptible – but in other cases, they would be.

Cox hopes that the delays on low-priority traffic will be minimal – on the order of milliseconds. If delays are limited to a tiny fraction of a second, the harm to the user should be minimal. However, queues any longer than a few seconds are significantly harmful to the normal operation of the Internet. Network applications generally treat packets as lost if an acknowledgement of receipt has not been received by the destination within a couple of seconds. With most applications, this causes the original sender to resend the packet. Additionally, routing protocols and devices often treat late packets as expired, and will drop them and wait for the sender to retransmit the data. If it takes too long for packets to be sent, the use of the queue will in fact generate additional congestion rather than limiting it. Cox's system can avoid a large queue delay by aggressively dropping old packets – but that also leads to retransmission of packets. The result could be both a highly inefficient network, and a frustrated user experience as a result of even longer delays.

Internet users and policymakers should monitor closely whether the trial run of this new DPI equipment produces more harm than good. Although it may reduce congestion in some circumstances and allow some applications to function better, putting some applications into a fast lane may cause other applications to work poorly or not at all. And because of packet retransmission, Cox's system may ultimately cause more congestion, rather than less. Finally, and most importantly, the user has no control over which of their applications are treated favorably and which unfavorably. Though consumers can give feedback to Cox and alert them to problems in the new system, the power to make changes will rest with Cox.

RISKS TO INNOVATION AND THE INTERNET

Cox's DPI technology marks a major shift in the operation of the Internet. Instead of consumers and application providers controlling traffic priority, the network itself makes the choice. Even assuming a perfectly innocent motive, DPI-enabled prioritization opens a Pandora's box of unintended consequences. First, moving control over content into the network destabilizes the market for applications and services by creating an artificial preference for one protocol or type of communication over others. Second, other unexpected problems may arise with user experiences under DPI-enabled prioritization because of varying uses of the same protocol or application by different users. Ultimately, if we accept the use of non-standard network management regimes that discriminate against specific applications, we risk a "balkanization" of the Internet – a world in which every ISP operates according to its own set of rules. The result would be a hodgepodge of different networks instead of one unified

and universal Internet, undermining the open platform and open market principles at the root of the Internet's success.

DPI-enabled prioritization puts innovation on the Internet at risk. Innovation in peer-to-peer protocols has resulted in valuable new applications and businesses – such as BitTorrent DNA, Vuze and P2P Next – based on the use of peer-to-peer for streaming video in particular. However, if all peer-to-peer traffic is labeled low priority, efforts by these companies to provide a superior video streaming experience will fail. Over time, application developers will steer clear of disfavored protocols and make services that do not run afoul of the latest network management tools. This would create an artificial pressure point in the market and misdirect innovation around barriers that have nothing to do with user choice. It also might force application providers to pay for priority access to avoid being deprioritized and to remain competitive. Finally, DPI-enabled prioritization might lead to an encryption arms race in which disfavored applications would encrypt all traffic to evade identification by DPI. Such an outcome would render the congestion-reduction purpose of DPI ineffective.

DPI-enabled prioritization also puts the user experience at risk. Consider the FTP protocol, declared by Cox to be “low priority.” One person may use FTP to upload a photo album from a recent vacation to a Web server to share with friends and family; another may use the protocol to upload real-time images of a security system. The former can fairly be considered “low priority,” but the latter cannot. The service provider, sitting in the middle of the network and using DPI to determine that the protocol in use is FTP, cannot make that distinction – only the user can. Over the Internet, the relative urgency of traffic is not best determined centrally, but by the host applications and users generating the traffic. If some traffic needs or deserves prioritized treatment, the technical standards underlying the Internet provide a way to do this, and to allow the user (rather than the network operator) to specify which traffic is important and which is not, through the use of DiffServ or IntServ. These methods have the additional advantage of not requiring the use of DPI, making the determination of priority faster and simpler.

It is easy to imagine a future when, in the pursuit of short-term benefits, network operators choose to implement dozens of different DPI tools that discriminate against certain types of applications. ISPs would apply a variety of tools based upon the particular characteristics of their networks, producing an environment in which content, services and applications function differently from ISP to ISP. Consider the example of Primus Telecommunications Canada. Primus has announced a network management system similar to Cox's, but using different classes and classifications of priority.²¹ Even if such a system seems reasonable as a response to an individual company's congestion problems, together, the varying systems of multiple ISPs would break the Internet into a collection of distinct networks. Such balkanization would place immense burdens on developers seeking to produce consistent and useful applications and services. Such an outcome would be disastrous not only for the user experience, but for all innovation and entrepreneurship on the Internet – a market that has always assumed an open platform where any application will work across the global network of networks.

Given the range and risk of harms, Internet users and policymakers alike should be wary of permitting a wide variety of DPI management tools to enter the market without scrutiny and investigation.

ZILLIONTV: THE FUTURE OF DISCRIMINATION?

Beyond the prioritization system employed by Cox, the future of discrimination on the Internet can be previewed today through ZillionTV. The ZillionTV service streams video programming over Internet access services directly to their subscribers, without the aid of any form of local storage or buffering – offering instant availability of content.²² Subscribers to ZillionTV purchase an inexpensive box (\$50), which may contain little more than an Internet port and a video decoder, and pay no subscription fees. They can then stream video programming content, for free, if they view a few minutes of advertisements per hour.²³

ZillionTV serves the same purpose as mainstream over-the-top video services such as Hulu or Netflix's on-demand technology, with one distinct difference. To support 2.7 Mbps streams without any substantial local caching while maintaining a steady, high-quality picture without glitches over current-generation broadband networks, ZillionTV requires assistance from ISPs.²⁴

As it turns out, this assistance may be substantial. For starters, the ZillionTV box will only be available for purchase through the ISP.²⁵ According to one source, the ISP must provide “dedicated bandwidth” that is “unaffected by any Net congestion that might degrade competing services.”²⁶ Similarly, another report claims, “Video wouldn’t actually traverse the public Internet; rather, ISP distributors would collocate VOD servers in their own facilities for optimal performance.”²⁷ Another article says that the ZillionTV deal with Hollywood studios and ISPs hinges on the delivery of video through ZillionTV faster than through Hulu or BitTorrent or other competing video delivery platforms.²⁸

It may be that ZillionTV will turn out to be nothing more than an add-on to cable TV service – a video product offered over the non-Internet portion of a local network. ZillionTV might use edge caching and might be able to operate without any prioritization or DPI. But their marketing blurs the lines, suggesting that ZillionTV may be transmitted over the Internet and gain advantages through DPI. The details remain murky, but the potential problem is clear: ZillionTV could work by claiming part of the Internet for its own use, and it would do so with the willing assistance of the ISP, which would assuredly be rewarded for the effort. And, ZillionTV has at least one major ISP already lined up as a customer.²⁹

ZillionTV's analysis of its own behavior is worthy of note. ZillionTV justifies prioritization of streaming video by citing Cox's network management trial, contending that streaming video has been recognized as a service that deserves extra “help.”³⁰ Notably, if ZillionTV were not traversing the Internet, it would not need the benefit of Cox's network management practices. ZillionTV has not yet officially launched its service, and some of its initial statements and reports appear contradictory. The alleged details of prioritization and established deals with ISPs have yet to be substantiated.

But if the ZillionTV business model relies on DPI-enabled prioritization, it represents the forefront of the next generation of discrimination on the Internet: carving out a portion of the once-neutral Internet for special treatment of its own traffic. And if ZillionTV succeeds over Netflix, Hulu and other competing services that operate over the “best efforts” Internet, it will have done so not because of superior technology or new ideas, but because it broke the neutrality and nondiscrimination of the Internet.

Regardless of the credibility of the system, ZillionTV's public messaging and the media attention it has garnered hint that an entire industry waits in the wings to use DPI and discrimination to transform the Internet into a mechanism to advance its business models. ZillionTV is the first of the dangers to peek out from the Pandora's box that will be opened if we allow DPI prioritization to operate unchecked.

THE FUTURE: MONITORING AND MONETIZING THROUGH DPI

Network operators and affiliated organizations seek to frame the Net Neutrality debate in terms of the need to manage congestion, to ensure that “fairness” exists among customers³¹ or to resolve emotionally charged issues like dialing 911 with a VoIP service.³² Although helpful in presenting the operators’ case to the public, these arguments disguise the true purpose of “network management,” which is to support new tools and business models based on real-time monitoring and control of Internet traffic.

These new tools and business models, including those of Comcast, NebuAd, Cox and ZillionTV, are enabled by abuses of DPI. In fact, an entire electronics industry has arisen as this technology has matured, creating equipment that is more affordable, efficient and sophisticated. These new devices have been developed and marketed for their capacity to enable ISPs to monitor and monetize the Internet.

DPI technology itself need not be anti-consumer if it is used to resolve congestion or security problems without harmful discrimination. But the value of DPI as marketed by prominent vendors derives instead from real-time monitoring and control of the Internet, uses that are explicitly contrary to the principles of an open Internet and to consumer choice.

MARKETING DPI TO INTERNET SERVICE PROVIDERS

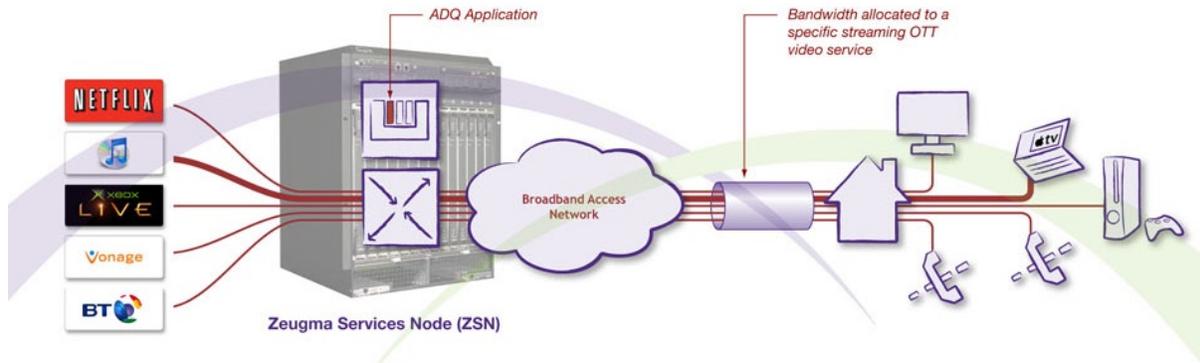
Marketing for DPI equipment extends well beyond private conversations with ISPs about the powers and pitfalls of the technology. Publicly available marketing materials and statements by manufacturers reveal that these devices are designed for ISPs to develop new methods to charge for individual uses of the Internet. Consider Andrew Harries, CEO of Zeugma Systems, a DPI equipment manufacturer: “Our view is that our customers’ most pressing concern is how to insert themselves into the over-the-top value chain,” he says.³³ Harries’ vision is to “enable our customers to see, manage and monetize individual flows to individual subscribers” – for example, “to deliver video quality over the Net, to either a PC or a TV, that convinces consumers to pay a little extra to the broadband service provider.”³⁴

A *Telephony Online* article describes Zeugma this way:

Zeugma enables service providers to sell QoS [Quality of Service] to content delivery networks such as Akamai, insert customer-specific advertising into content for advertisers, charge consumers for certain content and also get a percentage of sales from digital storefronts, as those increase over a higher performing network.³⁵

This elaborate marketing scheme is far from hypothetical. Zeugma partnered with Netflix and Roku to demonstrate how Zeugma technology could guarantee Netflix movies reach customers faster than other movie services. In one article, a Roku representative said a deal like this “gives broadband service providers an additional product that they can use to increase per-subscriber revenue.”³⁶ At the same time, the article observes, it “remains to be seen how consumers will react to paying extra for bandwidth they can already use now.”³⁷ Network operators seem keen on exploring DPI’s potential

to generate new sources of revenue. Prior to launching in May 2008, Zeugma had already established trials with two North American Tier-1 providers.³⁸



Source: Zeugma, <http://www.zeugmasystems.com/solutions/applicationdrivenqos/default.aspx>

Another DPI equipment manufacturer, Allot, published a marketing brochure touting its ability to increase ARPU (Average Revenue Per User) through “Tiered Services” and “Quota Management.”³⁹ Allot claims their equipment “enables quota-based service plans that allow providers to meter and control individual use of applications and services.”⁴⁰ Another Allot document states:

The platform delivers high performance, reliability, application awareness and subscriber awareness, which are key components for implementing solutions to control infrastructure and operating costs, and for deploying value added services to increase total and per-subscriber revenues (ARPU).⁴¹

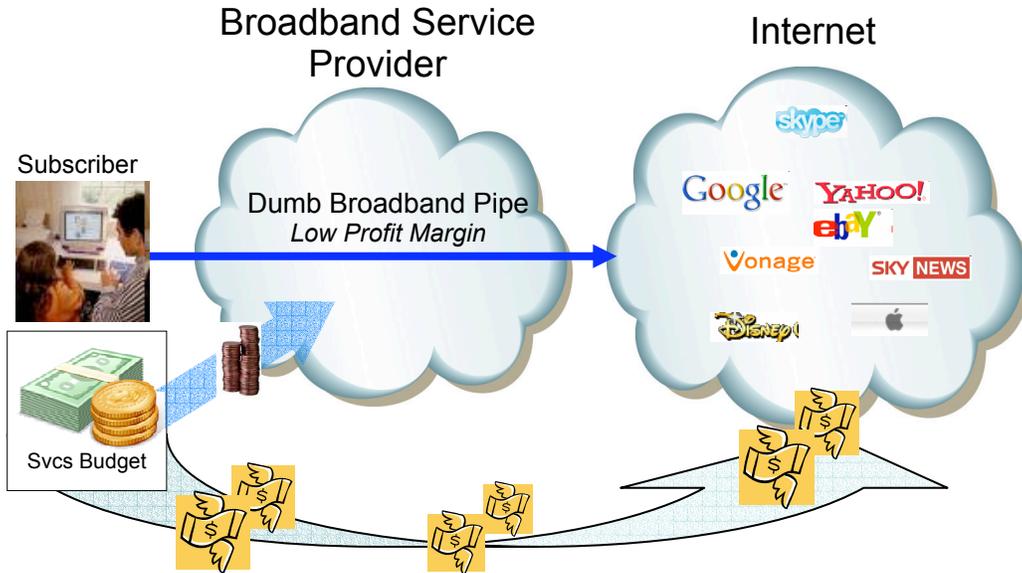
Allot created a tool that “enables service providers to project potential revenues and profits from setting up a tiered service infrastructure.”⁴² Even more blatantly, one of the “Service Provider Needs” listed by the company is to “reduce the performance of applications with negative influence on revenues (e.g. competitive VoIP services).”⁴³

Service Provider Needs
Have an accurate view of content and applications and who is using them
Improve the performance of applications with positive influence on revenues (e.g. churn reduction)
Reduce the performance of applications with negative influence on revenues (e.g. competitive VoIP services)
Manage ever-increasing volumes and types of traffic on the network

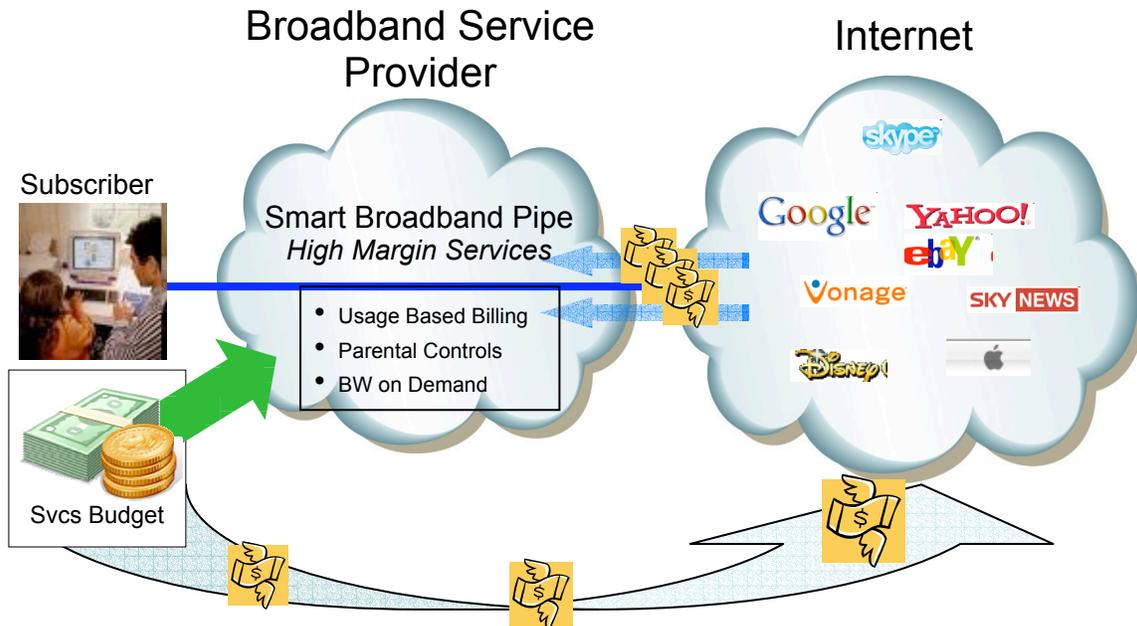
Source: Allot Communications, <http://www.sysob.com/download/AllotServiceGateway.pdf>

Camiant, another equipment manufacturer, similarly characterizes their “Multimedia Policy Engine” as “an intelligent platform for applying operator-defined business rules that determine which customers, tiers and/or applications receive bandwidth priority, at what charge and how much they may use.”⁴⁴

The firm's marketing has been effective – Camiant claims its DPI equipment “now reaches more than 70 percent of North American cable modem subscribers.”⁴⁵



Larger percentages of subscribers' budgets going to Internet Content



More Content Revenue Goes to the Broadband Service

Source: Network Strategy Partners, <http://0299d3f.netsolhost.com/NewPages/DPI.pdf>

Openet, whose clients include AT&T and Verizon, makes a similar value proposition to carriers:

In an era when subscriber acquisition rates are declining, the focus of service providers is on increasing profitability and competitiveness, which are largely dependent upon gaining visibility into and control over the events and transactions on their networks. In fact, network activity is a valuable resource that can be exploited to produce measurable business value by the savvy service providers that have the expertise and technology to extract that value from it.⁴⁶

Along these same lines, DPI firm Procera Networks markets a brochure titled, "If You Can See It, You Can Monetize It."⁴⁷ Procera recently boasted they had added 120 new customers in the second half of 2008.⁴⁸



Source: Procera, http://www.proceranetworks.com/images/documents/procera_brochure_web_0620.pdf

The latest DPI assessment from the industry publication *Light Reading* parrots the device manufacturers' claims: "Most important, [DPI] technology also offers service providers new ways of monetizing the traffic on their networks."⁴⁹ Similarly, Cisco Systems writes, "[B]y identifying services that might be riding an operator's network for free, a provider can truly differentiate its own 'branded' VoIP service traffic from best-effort traffic or extend QoS guarantees to that third party for a share of the profits."⁵⁰

DPI SHORTCHANGES CONSUMERS

Network providers can and will use DPI technology to improve their profits at the expense of their customers. The technology permits network operators to reduce the amount they spend on network upgrades by allowing them to oversell their networks while simultaneously increasing the amount the average customer pays, through the creation of new revenue streams.⁵¹ Or, in marketing language, providers want to "deliver customized service plans that increase customer satisfaction and reduce churn."⁵²

Yes, DPI can help alleviate problems of congestion in a network, thus improving the user experience. But the same DPI technology – the same electronics equipment, in fact – also allows providers to monitor and monetize every use of the Internet, and DPI vendors succeed by developing and marketing this capability. These DPI systems may already be installed in some operators' networks. A Yankee Group analyst asserts that U.S. ISPs are currently deploying advanced DPI equipment, although

many do not disclose it publicly.⁵³ Through these secret arrangements, the DPI industry is experiencing remarkable growth.⁵⁴

Precedent, motivation and capability all exist for providers of wireline and wireless Internet services to discriminate in the transmission of Internet content in search of new revenue streams. DPI now offers capabilities far beyond simply protecting Internet users from harm, and the service providers purchasing and installing DPI equipment are well aware of these possibilities.

If service providers flip the switch and turn on these control mechanisms, it might mean the end of the Internet as we know it.

ENDNOTES

- 1 47 U.S.C. § 202(a) (“It shall be unlawful for any common carrier to make any unjust or unreasonable discrimination in charges, practices, classifications, regulations, facilities, or services for or in connection with like communications service....”).
- 2 See generally *FCC Classifies Cable Modem Service as “Information Service”*, March 14, 2002, available at http://www.fcc.gov/Bureaus/Cable/News_Releases/2002/nrcb0201.html; *FCC Eliminates Mandated Sharing Requirement on Incumbents’ Wireline Broadband Internet Services*, Aug. 5, 2005, available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-260433A1.pdf.
- 3 *Appropriate Framework for Broadband Access to the Internet over Wireline Facilities; Review of Regulatory Requirements for Incumbent LEC Broadband Telecommunications Services; Computer III Further Remand Proceedings: Bell Operating Company Provision of Enhanced Services; 1998 Biennial Regulatory Review—Review of Computer III and ONA Safeguards and Requirements; Inquiry Concerning High-Speed Access to the Internet Over Cable and Other Facilities; Internet Over Cable Declaratory Ruling; Appropriate Regulatory Treatment for Broadband Access to the Internet Over Cable Facilities*, CC Docket Nos. 02-33, 01-337, 98-10, 95-20, GN Docket No. 00-185, CS Docket No. 02-52, Policy Statement, 20 FCC Rcd 14986 (2005) (*Internet Policy Statement*).
- 4 See *Comments of Free Press, et al., In the Matters of Free Press et al. Petition for Declaratory Ruling that Degrading an Internet Application Violates the FCC’s Internet Policy Statement and Does Not Meet an Exception for Reasonable Network Management; Broadband Industry Practices*, WC Docket No. 07-52 (Feb. 13, 2008), p. 29-34, Appendix 2, available at http://www.freepress.net/files/fp_et_al_comcast_petition_fp_comments.pdf.
- 5 See e.g., Jonathan Krim, “Executive Wants to Charge for Web Speed,” *Washington Post* (Dec. 1, 2005), available at <http://www.washingtonpost.com/wp-dyn/content/article/2005/11/30/AR2005113002109.html>; Paul Kapustka, “Verizon Says Google, Microsoft Should Pay for Internet Apps,” *InformationWeek* (Jan. 5, 2006), available at <http://www.informationweek.com/news/showArticle.jhtml?articleID=175801854>.
- 6 *Formal Complaint of Free Press and Public Knowledge Against Comcast Corporation for Secretly Degrading Peer-to-Peer Applications*, Free Press and Public Knowledge (Nov. 1, 2007), available at http://www.freepress.net/files/fp_pk_comcast_complaint.pdf; see also *Appropriate Framework for Broadband Access to the Internet over Wireline Facilities; Review of Regulatory Requirements for Incumbent LEC Broadband Telecommunications Services; Computer III Further Remand Proceedings: Bell Operating Company Provision of Enhanced Services, 1998 Biennial Review—Review of Computer III and ONA Safeguards and Requirements; Inquiry Concerning High-Speed Access to the Internet Over Cable and Other Facilities; Internet Over Cable Declaratory Ruling; Appropriate Regulatory Treatment for Broadband Access to the Internet Over Cable Facilities; Broadband Industry Practices*, CC Docket Nos. 02-33, 01-337, 95-20, 98-10, GN Docket No. 00-185, CS Docket No. 02-52, WC Docket No. 07-52, *Petition for Declaratory Ruling of Free Press, Public Knowledge, Media Access Project, Consumer Federation of America, Consumers Union, Information Society Project at Yale Law School, Professor Charles Nesson, Co-Director of the Berkman Center for Internet & Society, Harvard Law School, Professor Barbara van Schewick, Center for Internet & Society, Stanford Law School* (Nov. 1, 2007) (*Free Press Petition*), available at http://www.freepress.net/files/fp_et_al_nn_declaratory_ruling.pdf.
- 7 *In re Formal Complaint of Free Press & Public Knowledge Against Comcast Corp. for Secretly Degrading Peer-to-Peer Applications; Broadband Industry Practices; Petition of Free Press et al. for Declaratory Ruling That Degrading an Internet Application Violates the FCC’s Internet Policy Statement & Does Not Meet an Exception for “Reasonable Network Management,”* WC Docket No. 07-52, Memorandum Opinion and Order, FCC 08-183 (Aug. 20, 2008) (*Comcast Order*).
- 8 See e.g., Comcast Corporation, *Description of Planned Network Management Practices*, available at http://downloads.comcast.net/docs/Attachment_B_Future_Practices.pdf.
- 9 *Id.* at p. 11.
- 10 See *Letter from Ben Scott, Policy Director, Free Press to Marlene H. Dortch, Secretary, Federal Communications Commission*, File No. EB-08-IH-1518, WC Docket No. 07-52 (Oct. 14, 2008), available at http://fjallfoss.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6520175587.
- 11 See e.g., Ryan Singel, “Report: NebuAd Forges Packets, Violates Net Standards,” *Wired* (June 18, 2008), at <http://blog.wired.com/27bstroke6/2008/06/nebuad-forges-g.html>.

- 12 See Robb Topolski, Chief Technology Consultant, Free Press and Public Knowledge, *NebuAd and Partner ISPs: Wiretapping, Forgery and Browser Hijacking* (June 18, 2008), at http://www.freepress.net/files/NebuAd_Report.pdf.
- 13 *Id.* at 4.
- 14 "Charter hires NebuAd to make online ads more relevant," *IAB SmartBrief* (May 16, 2008), available at <http://www.smartbrief.com/news/iab/storyDetails.jsp?issueid=65693081-BF7F-4D7B-B0C4-B58D314EF624©id=75FCE22C-C5ED-4E05-B582-ED3970114D94&lmcid=>.
- 15 See e.g., Grant Gross, "Lawmakers Call on NebuAd to Change Privacy Notification," *PCWorld* (July 17, 2008), at http://www.pcworld.com/businesscenter/article/148555/lawmakers_call_on_nebuad_to_change_privacy_notification.html.
- 16 See e.g., Nate Anderson, "NebuAD CEO Defends Web Tracking, Tells Congress It's Legal," *Ars Technica* (July 9, 2008), at <http://arstechnica.com/news.ars/post/20080709-nebuad-ceo-defends-web-tracking-tells-congress-its-legal.html> ("Dorgan noted that neither he nor most consumers 'have the foggiest idea' about what's being tracked, how long it's maintained, and what it's being used for.").
- 17 Steven Musil, "Charter Drops Controversial Customer Tracking Plan," *CNET* (June 24, 2008), at http://news.cnet.com/8301-10784_3-9976893-7.html?tag=nefd.top.
- 18 See generally Comcast, *Frequently Asked Questions about Network Management*, available at <http://help.comcast.net/content/faq/Frequently-Asked-Questions-about-Network-Management> ("The new technique does not manage congestion based on the online activities, protocols or applications a customer uses, rather it only focuses on the heaviest users in real time, so the periods of congestion could be very fleeting and sporadic.").
- 19 See generally Cox Communications, *Congestion Management FAQs*, available at <http://www.cox.com/policy/congestionmanagement/>.
- 20 Though Cox claims to be able to maintain a lower bound on bandwidth for low-priority traffic, thus making this specific example unlikely.
- 21 "Primus Introduces New Internet Traffic Shaping System," *Digital Home* (March 18, 2009), available at <http://www.digitalhome.ca/content/view/3509/280/>.
- 22 Press Release, ZillionTV, *ZillionTV Corporation Unveils First-of-Its-Kind Television Service That Delivers on the Promise of Personalized TV* (March 4, 2009), available at <http://finance.yahoo.com/news/ZillionTV-Corporation-Unveils-bw-14538971.html>.
- 23 Eliot Van Buskirk, "ZillionTV: Hollywood and ISPs Unite to Deliver Video over the Net," *Wired* (March 4, 2009), at <http://blog.wired.com/business/2009/03/one-factor-that.html>.
- 24 Nate Anderson, "ZillionTV tempts net neutrality gods with prioritized video," *Ars Technica* (March 8, 2009), at <http://arstechnica.com/tech-policy/news/2009/03/zilliontv-tempts-net-neutrality-gods-with-prioritized-video.ars>.
- 25 Buskirk, *supra* note 23 ("This service's affiliation to ISPs is so strong, you won't be able to purchase a box anywhere but through your ISP, for a one-time activation fee of \$50.").
- 26 John Murrell, "Zillion? That's the eventual total of set-top box choices, right?," *Good Morning Silicon Valley* (Mar. 4, 2009), at <http://blogs.siliconvalley.com/gmsv/2009/03/zillion-thats-the-eventual-total-of-set-top-box-choices-right.html>.
- 27 Todd Spangler, "Look Like a Zillion Bucks?," *Multichannel News* (March 9, 2009), available at http://www.multichannel.com/article/189623-Look_Like_a_Zillion_Bucks_.php?rssid=20059.
- 28 Buskirk, *supra* note 23 ("Part of ZillionTV's partnership with both ISPs and Hollywood studios involves the ISPs delivering ZillionTV signals at higher speeds than those at which they deliver content from, say, Hulu or bit torrent, with whom they apparently have no such deal.").
- 29 Carol Wilson, "ZillionTV Creates a New On-Demand Video Option," *Telephony Online* (March 4, 2009), at http://telephonyonline.com/video/news/zillionTV_free_video_030409/?smtc=wl.
- 30 Buskirk, *supra* note 23 ("A couple of weeks ago, the Cox cable company put out an announcement regarding the matrix by which they're going to deal with those situations where their pipes are clogged," said [ZillionTV CEO Mitch] Berman. "It was a priority matrix of what they're going to do, and who they're going to help first. The first ones they say they're going to help are streaming, which is what we do.").

- 31 See e.g., Comments of National Cable & Telecommunications Association, *In the Matters of Formal Complaint of Free Press and Public Knowledge Against Comcast Corporation for Secretly Degrading Peer-to-Peer Applications*, File No. EB-08-IH-1518; Broadband Industry Practices, WC Docket No. 07-52, p. 3-5.
- 32 See e.g., Stephanie Condon, "Chamber Backs Broadband Deployment—without Net Neutrality Laws," *CNET* (Dec. 22, 2008), available at http://news.cnet.com/8301-13578_3-10128169-38.html; Grant Gross, "Net Neutrality Opponents Cite e-Health Efforts," *IDG News Service*, Aug. 15, 2007, available at http://www.pcworld.com/article/135949/net_neutrality_opponents_cite_ehealth_efforts.html.
- 33 Carol Wilson, "TelcoTV: Zeugma, Roku Team on Enhanced Net Video," *Telephony Online* (Nov. 13, 2008), available at <http://telephonyonline.com/iptv/news/enhanced-net-video-1113/>.
- 34 *Id.*
- 35 Carol Wilson, "Zeugma Aims to Redefine Edge," *Telephony Online* (May 27, 2008), at <http://telephonyonline.com/broadband/news/zeugma-redefine-edge-0527/index.html>.
- 36 Bob Wallace, "TelcoTV: Zeugma, Roku Demo QoE for Pay-Extra Services," *xchange*, available at <http://www.xchangemag.com/hotnews/zeugma-roku-demo-qoe-for-pay-extra-services.html>.
- 37 *Id.*
- 38 Wilson, *supra* note 35.
- 39 Allot Communications, *Subscriber Management Platform*, available at <http://www.ipnetworks-inc.com/pdfs/allot/Allot%20SMP%20Datasheet.pdf>.
- 40 *Id.*
- 41 Allot Communications, *Service Gateway*, available at http://www.cv-data.com/pdf/Service_Gateway.pdf.
- 42 Carol Wilson, "DPI Gets ROI Tool," *Light Reading* (Oct. 22, 2007), available at http://telephonyonline.com/broadband/technology/dpi_allot_yankee_102207/index.html.
- 43 Allot Communications, *Pushing the DPI Envelope* (June 2007), available at <http://www.sysob.com/download/AllotServiceGateway.pdf>.
- 44 Camiant, *Policy Server*, available at <http://www.camiant.com/products2.shtml>.
- 45 Camiant, *Camiant's PCMM-Qualified Policy Server Marks Major Milestone; Achieves over 70% Market Penetration* (Jan. 27, 2009), available at <http://www.camiant.com/press/p012709.shtml>. Camiant's customers include Comcast and Cox Communications. See Camiant, *Vodafone Hungary Deploys Camiant's Multimedia Policy Engine* (Jan. 21, 2009), available at <http://www.camiant.com/press/p012109.shtml>.
- 46 Openet, *Extracting Business Value at the Network Edge*, available at http://img.en25.com/Web/Openet/WP_Extracting_Business_Value_US_1008.pdf.
- 47 Procera Networks, *If You Can See It, You Can Monetize It*, available at http://www.proceranetworks.com/images/documents/procera_brochure_web_0620.pdf.
- 48 Procera Networks, *Explosive Adoption of Procera's PL10000 Platform* (Jan. 27, 2009), available at <http://www.proceranetworks.com/recent-press-releases/570-explosive-adoption-of-proceras-pl10000-platform.html>.
- 49 Simon Sherrington, "Deep Packet Inspection: Coming Soon to a Network Near You," *Light Reading* (Dec. 11, 2008), available at http://www.lightreading.com/document.asp?doc_id=169218.
- 50 Cisco Systems, *Deploying Premium Services Using Cisco Service Control Technology*, available at http://www.cisco.com/en/US/prod/collateral/ps7045/ps6129/ps6133/ps6150/prod_brochure0900aecd8025258e.pdf.
- 51 See e.g., Cloudshield Technologies, *Cloudshield Subscriber Services Manager*, available at http://www.cloudshield.com/applications/cs_ssm.asp ("By shaping traffic at the subscriber-level, bandwidth is made available for new revenue generating services. Rate limiting traffic allows network infrastructure build-out to be deferred, thereby reducing capital expenditures."); Arbor Networks, *Reduce Network Costs by Optimizing Bandwidth Utilization*, available at http://www.arbornetworks.com/index.php?option=com_docman&task=doc_download&gid=377 ("The ROI in the eSeries solution is achieved through cost reductions from reduced bandwidth purchases, deferred network infrastructure upgrades and improved customer support, plus new revenue associated with new service offerings").

- 52 Arbor Networks, *Arbor e100*, at <http://www.arbornetworks.com/en/arbor-ellacoya-e100.html>.
- 53 Wilson, *supra* note 42; see also Carol Wilson, "DPI: A Scorned Technology That's Thriving," *Light Reading* (July 21, 2008), available at <http://telephonyonline.com/iptv/news/dpi-scorned-but-thriving-0721/>.
- 54 Sherrington, *supra* note 49; see also Simon Sherrington, "The Greening of DPI," *Light Reading* (Nov. 19, 2007), available at http://www.lightreading.com/document.asp?doc_id=139389.